A. Shin
Filed 7/10/03
Q 76456
1 of 1

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　７月１０日

出願番号
Application Number: 特願２００２－２００９２０

[ST.10/C]: [ＪＰ２００２－２００９２０]

出願人
Applicant(s): 日本電気株式会社

２００３年　５月　６日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０３２９０３

【書類名】　特許願

【整理番号】　56200013PY

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/28

H04L 12/56

H04L 12/46

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　進　昭宏

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100083987

【弁理士】

【氏名又は名称】　山内　梅雄

【手数料の表示】

【予納台帳番号】　016252

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9006535

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ユーザ認証システムおよびユーザ認証方法

【特許請求の範囲】

【請求項１】　通信端末と、

この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、前記認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と

、

この物理ポート切替手段の未認証ポートから前記パケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与える一時使用アドレス提供手段と、

この一時使用アドレス提供手段の提供した一時使用ＩＰアドレスと通信端末の対応関係を記憶する一時使用ＩＰアドレス通信端末対応記憶手段と、

前記一時使用アドレス提供手段によって一時使用ＩＰアドレスの提供を受けた通信端末が前記所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が前記未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、

このログイン画面表示手段を使用して前記通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、

この認証可否判別手段が認証を行うと判別したとき前記一時使用ＩＰアドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用ＩＰアドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスを与えるネットワークアドレス付与手段

とを具備することを特徴とするユーザ認証システム。

【請求項２】　前記ネットワークアドレス付与手段によってネットワークアドレスを付与された前記通信端末がパケット信号を送出したときこれを前記認証

済ポートを経て受信し、これを該当する通信ネットワークに振り分けるネットワーク振り分け手段を具備することを特徴とする請求項１記載のユーザ認証システム。

【請求項３】　通信端末と、

この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、前記認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と、

この物理ポート切替手段の未認証ポートから前記パケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与える一時使用アドレス提供手段と、

この一時使用アドレス提供手段の提供した一時使用ＩＰアドレスと通信端末の対応関係を記憶する一時使用ＩＰアドレス通信端末対応記憶手段と、

前記一時使用アドレス提供手段によって一時使用ＩＰアドレスの提供を受けた通信端末が前記所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が前記未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、

このログイン画面表示手段を使用して前記通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、

この認証可否判別手段が認証を行うと判別したとき前記一時使用ＩＰアドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用ＩＰアドレスに代えて正規のＩＰアドレスを与える正規ＩＰアドレス付与手段

とを具備することを特徴とするユーザ認証システム。

【請求項４】　前記正規ＩＰアドレス付与手段によってＩＰアドレスを付与された前記通信端末がパケット信号を送出したときこれを前記認証済ポートを経

て受信し、これを該当するＩＰネットワークに振り分けるＩＰサブネット振り分け手段を具備することを特徴とする請求項３記載のユーザ認証システム。

【請求項５】　前記認証有無判別手段は認証を受けているユーザを登録したユーザ登録部を備え、このユーザ登録部に登録されているか否かによってユーザごとに認証が行われているか否かを判別することを特徴とする請求項１または請求項３記載のユーザ認証システム。

【請求項６】　前記ＩＰサブネット振り分け手段は、ＩＰアドレスと前記通信端末のＭＡＣアドレスのいずれかを用いて通信端末から送られてきたパケット信号の振り分けを行うことを特徴とする請求項４記載のユーザ認証システム。

【請求項７】　通信端末と、

この通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを与えるアドレス付与手段と、

このアドレス付与手段によって付与されたアドレスを使用して前記通信端末が認証を要求したとき、インターネットアクセス時に表示されるウェブ表示画面を認証用画面として認証のための入力操作および表示を行わせる認証時ウェブアクセス手段

とを具備することを特徴とするユーザ認証システム。

【請求項８】　前記ＩＰサブネット振り分け手段は、前記ＩＰアドレスとＭＡＣアドレスの双方が一致した宛先の通信ネットワークにパケット信号を振り分けることを特徴とする請求項４記載のユーザ認証システム。

【請求項９】　インターネットへのアクセスを行うに際してローカルエリアネットワークに接続されたネットワークサービスプロバイダに対して所定の通信端末からパケット信号を送出しインターネットへのアクセス要求を行うインターネットアクセス要求ステップと、

このインターネットアクセス要求ステップでインターネットへのアクセス要求があったときこの通信端末に対してログイン用の一時使用ＩＰアドレスを返送する一時使用ＩＰアドレス返送ステップと、

この一時使用ＩＰアドレス返送ステップで返送されてきた一時使用ＩＰアドレスを使用して前記通信端末から特定のインターネットサービスプロバイダに対す

る認証要求のパケット信号を送出する認証要求ステップと、

この認証要求ステップで送られてきたパケット信号に記された情報を基にして前記特定のインターネットサービスプロバイダの認証が得られるか否かをネットワークサービスプロバイダ側で判別する認証可否判別ステップと、

この認証可否判別ステップで認証が得られると判別したときその通信端末に対して前記特定のインターネットサービスプロバイダ用に割り当てられたＩＰアドレスを返送する正規ＩＰアドレス返送ステップと、

この正規ＩＰアドレス返送ステップで返送されてきた正規ＩＰアドレスを使用して前記通信端末からインターネットアクセス用のパケット信号を送出するインターネットアクセス用パケット信号送出ステップと、

このインターネットアクセス用パケット信号送出ステップで送出されたパケット信号を受信しその前記正規ＩＰアドレスを見てこれを前記特定のインターネットサービスプロバイダに振り分けるパケット信号振り分けステップ

とを具備することを特徴とするユーザ認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、たとえば複数のローカルエリアネットワークのいずれかを選択的に使用するユーザや、ＡＤＳＬ通信技術を使用してパケット信号を特定のインターネットサービスプロバイダを経由してインターネットに送出するユーザが、これらのネットワークに認証を行って接続するのに好適なユーザ認証システムおよびユーザ認証方法に関する。

【０００２】

【従来の技術】

通信設備の整備拡張に伴って、ＡＤＳＬ（Asymmetric Digital Subscriber Line）等のｘＤＳＬ（x Digital Subscriber Line）通信技術を使用して常時接続の環境でインターネットにアクセスすることが多くなっている。

【０００３】

図６は、ＡＤＳＬを使用してネットワークサービスプロバイダに接続する従来

の通信システムの概要を表わしたものである。この通信システム１００で、パーソナルコンピュータからなる通信端末１０１はモデム（変復調装置）１０２を介してブロードバンドアクセスサーバ（ＢＡＳ：Broadband Access Server）１０３と接続されている。ブロードバンドアクセスサーバ１０３は、ＡＤＳＬ等のｘＤＳＬあるいはＦＴＴＨ（Fiber To The Home）等の高速なインターネット常時接続サービスを提供するために、図示しない通信局舎内に設置されるサーバをいう。ブロードバンドアクセスサーバ１０３は、通常の場合、複数のインターネットサービスプロバイダ（ＩＳＰ：Internet Service Provider）104_1、104_2、……を介して図示しないインターネット網に接続されている。

【０００４】

このような通信システム１００では、ポイントツーポイントプロトコル・オーバ・イーサネット（登録商標）（ＰＰＰｏＥ：Point To Point Protocol over Ethernet（登録商標））セッション１０５を使用して、通信端末１０１からブロードバンドアクセスサーバ１０３までポイントツーポイントデータを転送するようにしている。ここでこのポイントツーポイント・オーバ・イーサネット（登録商標）プロトコルは２点間を接続してデータ通信を行うためのプロトコルである。このプロトコルを使用することでＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）を始めとする多くのプロトコルを中継することができる。ここでは、イーサネット（登録商標）等のローカルエリアネットワークで、ＩＰアドレスを組み込んだパケット信号をカプセル化してブロードバンドアクセスサーバ１０３に転送するためにポイントツーポイントプロトコルセッション１０５が使用される。たとえば特開平１０－１７３６９１号公報にこの種の技術が開示されている。

【０００５】

ブロードバンドアクセスサーバ１０３はローカルエリアネットワーク上を通信端末１０１から送られてきた信号をデカプセル化してパケット信号を取り出し、通信端末１０１が契約したインターネットサービスプロバイダ104_Xにこれを転送する。インターネットサービスプロバイダ104_Xは通信端末１０１に対してパスワードを要求する等の手法で本人確認としての認証を行い、これが成功し

たら通信端末１０１から送られてきたパケット信号をそのＩＰアドレスの示す相手先に送出することになる。

【０００６】

このように、この図６に示した通信システム１００では、通信端末１０１がインターネットサービスプロバイダ１０４$_X$に直接接続されていれば本来必要としないポイントツーポイントプロトコルを使用してパケット信号をカプセル化して転送している。このためブロードバンドアクセスサーバ１０３はポイントツーポイントプロトコルによるヘッダの取り付けや取り外しといったパケット信号のカプセル化やデカプセル化の作業を必要とする。現在、インターネットへの常時接続の環境が急速に整ってきており、これに伴って加入者端末１０１がその契約した特定のインターネットサービスプロバイダ１０４$_X$を通して通信するパケット信号の量が増加している。また、常時接続に適したアプリケーションソフトウェアの登場やウェブサイトの増加によって、今後、ますます加入者端末１０１とインターネットサービスプロバイダ１０４$_X$の間の通信量が増加することは確実である。このような状況の下では、ポイントツーポイントプロトコルを使用したパケット信号のカプセル化あるいはカプセルを取り除くデカプセル化の作業を撤廃あるいは軽減する必要がある。

【０００７】

図７は、以上説明したポイントツーポイントプロトコルを使用しないで済む従来提案された通信システムの概要を表わしたものである。この図７で図６と同一部分には同一の符号を付しており、これらの説明を適宜省略する。この通信システム１２０では、通信端末１０１がＶＬＡＮ（Virtual Local Area Network）スイッチ１２１に接続されている。ＶＬＡＮスイッチ１２１は、バーチャル・ローカルエリアネットワーク１２２$_1$、１２２$_2$、……によって複数のインターネットサービスプロバイダ（ＩＳＰ：Internet Service Provider）１０４$_1$、１０４$_2$、……を介して図示しないインターネット網に接続されている。したがって、通信端末１０１がインターネットサービスプロバイダ１０４$_X$とインターネットの接続について契約を行っているものとすると、ＶＬＡＮスイッチ１２１は通信端末１０１がログインすると認証を行い、認証が成功すれば契約先のインターネッ

トサービスプロバイダ１０４$_X$と接続する。なお、ＶＬＡＮについては特開平０９－１３０４２１号公報等に開示がある。

【０００８】

【発明が解決しようとする課題】

この図７に示した通信システム１２０では、図６で説明したようなポイントツーポイントプロトコルを使用する必要がない。したがって、プロトコルスタック数が多すぎるためにブロードバンド化という観点から、既存の設備としてのブロードバンドアクセスサーバ１０３やルータがボトルネックとなるという問題から開放される。また、認証が終わった後にはバーチャルなローカルエリアネットワークとしてのバーチャル・ローカルエリアネットワーク１２２$_1$、１２２$_2$、……に接続されるので、スループットの点で大幅な改善が期待される。

【０００９】

しかしながら、この通信システム１２０ではバーチャル・ローカルエリアネットワークを採用している。このため、ＶＬＡＮスイッチ１２１が分岐できるバーチャル・ローカルエリアネットワークの数は、バーチャル・ローカルエリアネットワークを転送されるフレームのＶＬＡＮフィールドが１２ビット構成となっていることから、２の１２乗個、すなわち４０９６個が最大となっている。ローカルエリアネットワークはたとえば１つの企業内でも部署や物理的な位置に応じて多数組まれる場合があり、これらを集合して更に大きなネットワークを構成していったとき、この制限は通信システムの構築に大きな制約となる。

【００１０】

そこで本発明の目的は、通信端末がローカルエリアネットワークを介して自在に通信ネットワークや所望のローカルエリアネットワークに数の制約なく接続することのできるユーザ認証システムおよびユーザ認証方法を提供することにある。

【００１１】

【課題を解決するための手段】

請求項１記載の発明では、（イ）通信端末と、（ロ）この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で

入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記した所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と、（ハ）この物理ポート切替手段の未認証ポートからパケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与える一時使用アドレス提供手段と、（ニ）この一時使用アドレス提供手段の提供した一時使用ＩＰアドレスと通信端末の対応関係を記憶する一時使用ＩＰアドレス通信端末対応記憶手段と、（ホ）一時使用アドレス提供手段によって一時使用ＩＰアドレスの提供を受けた通信端末が前記した所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、（ヘ）このログイン画面表示手段を使用して通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、（ト）この認証可否判別手段が認証を行うと判別したとき一時使用ＩＰアドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用ＩＰアドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスを与えるネットワークアドレス付与手段とをユーザ認証システムに具備させる。

【００１２】

すなわち請求項１記載の発明では、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力するようになっている。そして、これが認証済であるかどうかを判別し、認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与えるようにしている。一時使用ＩＰアドレスを受け取った通信端末は、これを用いてパケット信号を送出し物理ポート切替手段の未認証ポートを経てログイン画面表示手段に入力され、ログイン画面の表示が行われる。通信端末はログイン画面で認証のためのログインを行い、認証可否判別

手段が認証を行うか否かを判別する。認証が成功した場合には一時使用ＩＰアドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスが与えられる。したがって、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。ネットワークアドレスの数は前記したＶＬＡＮフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、ネットワークアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【００１３】

請求項２記載の発明では、請求項１記載のユーザ認証システムは、ネットワークアドレス付与手段によってネットワークアドレスを付与された通信端末がパケット信号を送出したときこれを認証済ポートを経て受信し、これを該当する通信ネットワークに振り分けるネットワーク振り分け手段を具備することを特徴としている。

【００１４】

すなわち請求項２記載の発明では、ネットワーク振り分け手段がネットワークアドレスによって通信端末が送出したパケット信号の振り分けを行うことにしている。

【００１５】

請求項３記載の発明では、（イ）通信端末と、（ロ）この通信端末から認証を要する所定の通信ネットワークに対して送り出されたパケット信号をその手前で入力するパケット信号入力手段と、このパケット信号入力手段が入力したパケット信号が前記した所定の通信ネットワークに認証を受けたものであるか否かを判別する認証有無判別手段と、この認証有無判別手段が未認証と判別したときこれを出力する未認証ポートと、認証有無判別手段が認証済と判別したときこれを出力する認証済ポートとを備えた物理ポート切替手段と、（ハ）この物理ポート切替手段の未認証ポートからパケット信号が出力されたとき、そのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与える一時使用アドレス提供手段と、（ニ）この一時使用アドレス提供手段の提供した

一時使用ＩＰアドレスと通信端末の対応関係を記憶する一時使用ＩＰアドレス通信端末対応記憶手段と、（ホ）一時使用アドレス提供手段によって一時使用ＩＰアドレスの提供を受けた通信端末が前記した所定の通信ネットワークに対して認証を受けるためにログインしそのパケット信号が未認証ポートから出力されたときこれを入力してログイン画面を表示するログイン画面表示手段と、（ヘ）このログイン画面表示手段を使用して通信端末からログインが行われたときこれに対して認証を行うか否かを判別する認証可否判別手段と、（ト）この認証可否判別手段が認証を行うと判別したとき一時使用ＩＰアドレス通信端末対応記憶手段に記憶された通信端末に対応させる形でこれに対して一時使用ＩＰアドレスに代えて正規のＩＰアドレスを与える正規ＩＰアドレス付与手段とをユーザ認証システムに具備させる。

【００１６】

すなわち請求項３記載の発明では、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力するようになっている。そして、これが認証済であるかどうかを判別し、認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与えるようにしている。一時使用ＩＰアドレスを受け取った通信端末は、これを用いてパケット信号を送出し物理ポート切替手段の未認証ポートを経てログイン画面表示手段に入力され、ログイン画面の表示が行われる。通信端末はログイン画面で認証のためのログインを行い、認証可否判別手段が認証を行うか否かを判別する。認証が成功した場合には一時使用ＩＰアドレスに代えて認証の対象となった所望の通信ネットワークに転送するための正規のＩＰアドレスが与えられる。したがって、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。ＩＰアドレスによって特定される宛先の数は無制限に近い数まで可能であり、前記したＶＬＡＮフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、ＩＰアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【００１７】

請求項４記載の発明では、請求項３記載のユーザ認証システムは、正規ＩＰアドレス付与手段によってＩＰアドレスを付与された通信端末がパケット信号を送出したときこれを認証済ポートを経て受信し、これを該当するＩＰネットワークに振り分けるＩＰサブネット振り分け手段を具備することを特徴としている。

【００１８】

すなわち請求項４記載の発明では、ＩＰサブネット振り分け手段がＩＰパケットのサブネットアドレスによって通信端末が送出したパケット信号の振り分けを行うことにしている。

【００１９】

請求項５記載の発明では、請求項３記載のユーザ認証システムで、認証有無判別手段は認証を受けているユーザを登録したユーザ登録部を備え、このユーザ登録部に登録されているか否かによってユーザごとに認証が行われているか否かを判別することを特徴としている。

【００２０】

すなわち請求項５記載の発明では、認証前のパケット信号について認証を行う必要があるので認証有無判別手段でユーザ登録部を用いてその判別を行うようにしている。ユーザ登録部は認証されているユーザを登録しておりこれを検索することで認証の有無を判別することができる。ユーザの特定は、たとえばＭＡＣアドレスを用いて行うことができる。

【００２１】

請求項６記載の発明では、請求項４記載のユーザ認証システムで、ＩＰサブネット振り分け手段は、ＩＰアドレスと通信端末のＭＡＣアドレスのいずれかを用いて通信端末から送られてきたパケット信号の振り分けを行うことを特徴としている。

【００２２】

すなわち請求項６記載の発明では、ＩＰサブネット振り分け手段の振り分けの態様を規定している。ＩＰアドレスを振り分け先の通信ネットワークにそれぞれ対応付けて用意しておけば、ＩＰアドレスを調べるだけでどの通信ネットワーク

に振り分けるかを判別することができる。これ以外に通信端末のＭＡＣアドレスを用いて振り分けを行うことも可能である。このように振り分けについて２種類の情報を使い分けることで、パケット信号の振り分けを、個々のユーザに与えるＩＰアドレスによってあるいはハードウェア自体によって異なった観点から行うことができる。

【００２３】

請求項７記載の発明では、（イ）通信端末と、（ロ）この通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを与えるアドレス付与手段と、（ハ）このアドレス付与手段によって付与されたアドレスを使用して通信端末が認証を要求したとき、インターネットアクセス時に表示されるウェブ表示画面を認証用画面として認証のための入力操作および表示を行わせる認証時ウェブアクセス手段とをユーザ認証システムに具備させる。

【００２４】

すなわち請求項７記載の発明では、アドレス付与手段が通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを、とりあえず与えることにしている。そして、この通信端末が与えられたアドレスを用いて認証を要求してきたときには、認証時ウェブアクセス手段がインターネットアクセス時に表示されるウェブ表示画面を認証用画面として認証のための入力操作および表示を行わせることにしている。このようにウェブ表示画面を用いて認証の手続きを行うので、通信端末に特別な認証用のアプリケーションソフトウェアをインストールすることなく、通常備わっているブラウザを使用して認証のための操作が可能である。

【００２５】

請求項８記載の発明では、請求項４記載のユーザ認証システムで、ＩＰサブネット振り分け手段は、ＩＰアドレスとＭＡＣアドレスの双方が一致した宛先の通信ネットワークにパケット信号を振り分けることを特徴としている。

【００２６】

すなわち請求項８記載の発明では、請求項４記載のユーザ認証システムで、ＩＰサブネット振り分け手段は、ＩＰアドレスとＭＡＣアドレスの双方が一致した

場合を扱っている。このように両者が一致する場合で振り分け先を決めることでセキュリティを高めることが可能になる。

【００２７】

請求項９記載の発明では、（イ）インターネットへのアクセスを行うに際してローカルエリアネットワークに接続されたネットワークサービスプロバイダに対して所定の通信端末からパケット信号を送出しインターネットへのアクセス要求を行うインターネットアクセス要求ステップと、（ロ）このインターネットアクセス要求ステップでインターネットへのアクセス要求があったときこの通信端末に対してログイン用の一時使用ＩＰアドレスを返送する一時使用ＩＰアドレス返送ステップと、（ハ）この一時使用ＩＰアドレス返送ステップで返送されてきた一時使用ＩＰアドレスを使用して通信端末から特定のインターネットサービスプロバイダに対する認証要求のパケット信号を送出する認証要求ステップと、（ニ）この認証要求ステップで送られてきたパケット信号に記された情報を基にして前記した特定のインターネットサービスプロバイダの認証が得られるか否かをネットワークサービスプロバイダ側で判別する認証可否判別ステップと、（ホ）この認証可否判別ステップで認証が得られると判別したときその通信端末に対して前記した特定のインターネットサービスプロバイダ用に割り当てられたＩＰアドレスを返送する正規ＩＰアドレス返送ステップと、（ヘ）この正規ＩＰアドレス返送ステップで返送されてきた正規ＩＰアドレスを使用して通信端末からインターネットアクセス用のパケット信号を送出するインターネットアクセス用パケット信号送出ステップと、（ト）このインターネットアクセス用パケット信号送出ステップで送出されたパケット信号を受信しその正規ＩＰアドレスを見てこれを前記した特定のインターネットサービスプロバイダに振り分けるパケット信号振り分けステップとをユーザ認証方法に具備させる。

【００２８】

すなわち請求項９記載の発明では、インターネットへのアクセスを行うのに際してローカルエリアネットワークに接続されたネットワークサービスプロバイダに対して所定の通信端末からパケット信号を送出し、インターネットへのアクセス要求を行い、ネットワークサービスプロバイダ側からログイン用の一時使用Ｉ

Ｐアドレスを返送してもらう。そして、この一時使用ＩＰアドレスを使用して通信端末から特定のインターネットサービスプロバイダに対する認証要求のパケット信号を送出して（認証要求ステップ）、このパケット信号に記された情報を基にして前記した特定のインターネットサービスプロバイダの認証が得られるか否かをネットワークサービスプロバイダ側で判別させる（認証可否判別ステップ）。この認証可否判別ステップで認証が得られると判別されたときには、その通信端末に対してネットワークサービスプロバイダ側から前記した特定のインターネットサービスプロバイダ用に割り当てられたＩＰアドレスが正規アドレスとして返送される（正規ＩＰアドレス返送ステップ）。この場合には、この正規ＩＰアドレスを使用して通信端末からインターネットアクセス用のパケット信号がネットワークサービスプロバイダ側に送出されると（インターネットアクセス用パケット信号送出ステップ）、ネットワークサービスプロバイダ側ではこのパケット信号の正規ＩＰアドレスを見てこれを前記した特定のインターネットサービスプロバイダ側に振り分けることができる（パケット信号振り分けステップ）。したがって、それ以後は所望の通信ネットワークとの通信が可能になる。ＩＰアドレスの数は前記したＶＬＡＮフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、ＩＰアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【００２９】

【発明の実施の形態】

【００３０】

【実施例】

以下実施例につき本発明を詳細に説明する。

【００３１】

＜第１の実施例＞

【００３２】

図１は本発明の第１の実施例におけるユーザ認証システムを表わしたものである。このユーザ認証システム２００で、加入者端末２０１はイーサネット（登録

商標）（Ethernet（登録商標））等のネットワーク（以下、ローカルエリアネットワークと称する。）２０２と接続されている。このローカルエリアネットワーク２０２は、ネットワークサービスプロバイダ（ＮＳＰ：Network Service Provider）２０３内に位置する物理ポートの切り替えを行う物理ポート切替スイッチ２０４の入力側と接続されている。物理ポート切替スイッチ２０４は認証済の物理ポートに対応する認証ポート２０５と、認証が行われていない物理ポートに対応する未認証ポート２０６の２つのポートの切り替えを行うスイッチである。認証ポート２０５は、ユーザの認証が行われた後のＩＰパケットを転送する認証ＩＰネットワーク２０７に接続されている。

【００３３】

認証ＩＰネットワーク２０７は、本実施例の場合、ＩＰパケットをサブネットによって第１のインターネットサービスプロバイダ（ＩＳＰ：Internet Service Provider）208_1あるいは第２のインターネットサービスプロバイダ208_2のうちの一方の経路に振り分けて送信するＩＰサブネット振分スイッチ２０９に接続されている。ＩＰアドレスはネットワークアドレスとホストアドレスの２つに分けられるが、そのうち、ネットワークアドレスをさらに分割したものがサブネットワークアドレスである。ＩＰサブネット振分スイッチ２０９は、ＩＰアドレスにおけるサブネットワークアドレスを見て、第１のターゲットＩＰネットワーク214_1のネットワークアドレスと一致していれば、加入者端末２０１から送出されたフレーム信号を、第１のターゲットＩＰネットワーク214_1にフォワード（転送）する。これに対して、第２のターゲットＩＰネットワーク214_2のネットワークアドレスと一致していれば、このフレーム信号を第２のターゲットＩＰネットワーク214_2にフォワードすることになる。

【００３４】

また、認証ＩＰネットワーク２０７は、加入者端末２０１の認証を行うための認証ＩＰネットワークＤＨＣＰサーバ２１１の一端と接続されている。ここで、ＤＨＣＰ（Dynamic Host Configuration Protocol）とは、各ユーザに、起動時に動的にＩＰアドレスを割り当て、終了時にこのＩＰアドレスを回収するためのプロトコルである。認証ＩＰネットワークＤＨＣＰサーバ２１１は、物理ポート

切替スイッチ２０４から送られてきた送信元のＭＡＣアドレスを第１および第２のＲＡＤＩＵＳ（Remote Authentication Dialin User Service）サーバ２１３$_1$、２１３$_2$のうちの該当するもの、すなわち認証の対象となるインターネットサービスプロバイダ２０８を担当する者に渡してＩＰアドレスを受け取り、これを加入者端末２０１に割り当てる役割をもっている。第１および第２のＲＡＤＩＵＳサーバ２１３$_1$、２１３$_2$のうち該当するものは、クライアントからのダイアルアップ接続認証要求を受けて、認証の可否をクライアントに返すようになっている。認証ＩＰネットワークＤＨＣＰサーバ２１１の他端は、このユーザ認証システム２００でユーザの認証のための管理に使用される管理用ＩＰネットワーク２１２と接続されている。

【００３５】

一方、物理ポート切替スイッチ２０４の未認証ポート２０６側には、未認証のパケット信号を入力して認証のための処理を行うためのデフォルトＩＰネットワーク２１７が接続されている。このデフォルトＩＰネットワーク２１７には、未認証のパケット信号をログインさせるためのログイン用ウェブサーバ２１５とデフォルトＩＰネットワーク用ＤＨＣＰ（Dynamic Host Configuration Protocol）サーバ２１６のそれぞれ一端が接続されている。ここで、ログイン用ウェブサーバ２１５は、特別なソフトウェアをインストール必要なく、一般にパーソナルコンピュータの購入時等に付属している使用料が不要あるいは安価なウェブページ閲覧用のソフトウェアを使用してログインさせるためのものである。デフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６は、再利用可能なＩＰアドレスの動的割り当てを行うためのサーバであり、具体的にはログイン用ウェブサーバ２１５でログインを行わせるために臨時にＩＰアドレスを与えるサーバである。これらログイン用ウェブサーバ２１５およびデフォルトＤＨＣＰサーバ２１６は管理用ＩＰネットワーク２１２とも接続されている。

【００３６】

管理用ＩＰネットワーク２１２は、前記した認証ＩＰネットワークＤＨＣＰサーバ２１１と接続している他に、第１および第２のＲＡＤＩＵＳサーバ２１３$_1$、２１３$_2$とも接続している。これらＲＡＤＩＵＳサーバ２１３$_1$、２１３$_2$は、

加入者端末２０１からのダイアルアップ接続認証要求を受けて、認証の可否をクライアントに返す役割を持っている。また、第１のＲＡＤＩＵＳサーバ２１３$_1$は、加入者端末２０１が第１のターゲットＩＰネットワーク２１４$_1$および第１のインターネットサービスプロバイダ２０８$_1$を経てインターネット網に接続するものであれば、このような振分けを可能とするＩＰアドレスをこれに与えるようになっている。これに対して、加入者端末２０１が第２のターゲットＩＰネットワーク２１４$_2$および第２のインターネットサービスプロバイダ２０８$_2$を経てインターネット網に接続するものである場合には、このような振分けを可能とするＩＰアドレスをこれに与えることになる。

【００３７】

ところで本実施例のユーザ認証システム２００で物理ポート切替スイッチ２０４はローカルエリアネットワーク２０２を経てネットワークサービスプロバイダ２０３に加入者端末２０１側から送られてきたパケット信号を受信する。そしてそのパケット信号の送信元のＭＡＣ（Media Access Control）アドレスを調べ、これに応じてポートの切替制御を行うようになっている。

【００３８】

図２は、この物理ポート切替スイッチの制御の様子を表わしたものである。図１に示した物理ポート切替スイッチ２０４は、図示しないがＣＰＵ（中央処理装置）、制御プログラムを格納する記憶媒体、出力ポートを切り替える切替手段ならびにＭＡＣアドレスを登録するＭＡＣアドレス登録テーブルを備えている。物理ポート切替スイッチ２０４はパケット信号が到来すると（ステップＳ３０１：Ｙ）、そのＭＡＣアドレスを判別する（ステップＳ３０２）。ＭＡＣアドレスは、ＮＩＣ(Network Interface Card)ごとに割り当てられる番号であり、６オクテットで表わされている。そしてこのＭＡＣアドレスと同一のアドレスがＭＡＣアドレス登録テーブルに登録されているか検索する（ステップＳ３０３）。

【００３９】

本実施例のＭＡＣアドレス登録テーブルには、ユーザ認証を受けたＭＡＣアドレスを登録するようにしている。ただし、一度登録を行ったＭＡＣアドレスであってもログアウトした時点でその登録内容は消去されるようになっている。物理

ポート切替スイッチ２０４内の前記したＣＰＵは受信したパケット信号のＭＡＣアドレスがＭＡＣアドレス登録テーブルに登録されているものであれば（ステップＳ３０４：Ｙ）、物理ポートを認証ポート２０５側に切り替えて（ステップＳ３０５）、そのパケット信号を図１に示す認証ＩＰネットワーク２０７へ送り出す。

【００４０】

これに対して、受信したパケット信号のＭＡＣアドレスがＭＡＣアドレス登録テーブルに登録されていない場合には（ステップＳ３０４：Ｎ）、物理ポートを未認証ポート２０６側に切り替えて（ステップＳ３０６）、そのパケット信号を図１に示すデフォルトＩＰネットワーク２１７へ送り出すことになる。

【００４１】

今、図１に示した加入者端末２０１のユーザが第１のインターネットサービスプロバイダ２０８_1とインターネット網の接続について契約を行っているものとする。このユーザが、インターネットにアクセスするために所定の時点で加入者端末２０１のブラウザを立ち上げて第１のインターネットサービスプロバイダ２０８_1に対する認証要求のための処理を開始したものとする。これにより加入者端末２０１から送出されたパケット信号は、第１のインターネットサービスプロバイダ２０８_1の手前に配置されたネットワークサービスプロバイダ２０３の物理ポート切替スイッチ２０４に入力される。物理ポート切替スイッチ２０４はこの認証がまだ行われていない時点で加入者端末２０１のＭＡＣアドレスをＭＡＣアドレス登録テーブルに登録していない。そこで、ユーザ認証を行うためのユーザのログインを可能とする仮のＩＰアドレスを与える手続きに入ることになる。

【００４２】

図３は、本実施例のユーザ認証システムの原理的な構成を示したものである。ユーザ認証システム２００の主要部を構成するネットワークサービスプロバイダ２０３は、ローカルエリアネットワーク２０２を通じてパケット信号４０１を物理ポート切替スイッチ２０４に入力する。このとき、まだ所定のインターネットサービスプロバイダ２０８との間でインターネットの接続を行うための認証が行われていないので、物理ポート切替スイッチ２０４はユーザ認証手段４０２と接

続し、ユーザ認証の手続きを開始する。この手続きでユーザ認証が成功すると、ネットワークサービスプロバイダ２０３はその加入者端末２０１にＩＰアドレスを与える。このときＩＰサブネットアドレス払出手段４０３はネットワークサービスプロバイダ２０３側が予め貯蔵しておいたＩＰアドレスの中から１つをその加入者端末２０１用に払い出す。これについては後に具体的に説明する。

【００４３】

この後、加入者端末２０１が送出したパケット信号には、ネットワークサービスプロバイダ２０３側でその払い出されたＩＰアドレスが使用される。これにより、物理ポート切替スイッチ２０４から認証ＩＰネットワーク２０７へ送り出されたパケット信号は、後に詳細を説明するＩＰアドレスＭＡＣアドレスフィルタ手段４０４に入力されてフィルタリングされ、振分手段４０５でＩＰサブネットワークを見て特定のインターネットサービスプロバイダ２０８あるいは図示しない通信ネットワークに振り分けられることになる。ユーザの振分けとしてのフィルタリングはＩＰアドレスによって行うこともＭＡＣアドレスによって行うことも可能である。両者の組み合わせによってもよい。

【００４４】

さて、以上の概略の説明の後に、再びユーザ認証手段４０２の処理の箇所から具体的な説明を行う。ユーザがインターネットに接続するために加入者端末２０１を操作すると、加入者端末２０１からＩＰアドレスを取得するためにＤＨＣＰリクエストパケットが送出される。

【００４５】

図４は、ＤＨＣＰリクエストパケットが送出された時点以降の本実施例のユーザ認証システムにおける加入者端末側の処理の概要を表わしたものである。図１と共にこれを説明する。加入者端末２０１はＤＨＣＰリクエストパケットをブロードキャストフレームで送信する（ステップＳ５０１）。物理ポート切替スイッチ２０４はこれを受信すると未認証ポート２０６に接続されたデフォルトＩＰネットワーク２１７にフォワードする。

【００４６】

デフォルトＩＰネットワーク２１７に収容されているデフォルトＩＰネットワ

ーク用ＤＨＣＰサーバ２１６は、加入者端末２０１から送られてきたＤＨＣＰリクエストパケットを受け取る。そして、受け取ったことを示す“ａｃｋ”信号を返送する。したがって、加入者端末２０１はこの“ａｃｋ”信号を受信するまで（ステップＳ５０２：Ｎ）、ＤＨＣＰリクエストパケットの送出を繰り返すことになる。

【００４７】

デフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６はこの“ａｃｋ”信号を返送するが、このとき加入者端末２０１に対して予め用意した未使用のＩＰアドレスを付加して送信する。この結果として、加入者端末２０１はＤＨＣＰリクエストパケットの受信を意味する“ａｃｋ”信号を受信したら（ステップＳ５０２：Ｙ）、次に臨時に割り当てられたこのＩＰアドレスを取得することになる（ステップＳ５０３）。この臨時のＩＰアドレスを割り当てたとき、デフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６は、加入者端末２０１のＭＡＣアドレスと、このＭＡＣアドレスに割り当てたＩＰアドレスをその図示しない記憶領域に記憶しておく。また、このとき割り当てるＩＰアドレスは有限な時間でリースされるものであるため、リース時間ｔを設定する。一例としては、リース時間ｔを５秒程度に設定する。もちろん、リース時間ｔは１時間といったように、これより長い時間であってもよい。

【００４８】

このようにしてＩＰアドレスが一時的に割り当てられると、加入者端末２０１はそのウェブ（ＷＥＢ）ブラウザを用いてログイン用ウェブサーバ２１５にアクセスする。ログイン用ウェブサーバ２１５は、“ｈｔｔｐ”（hypertext transfer protocol）手順でユーザＩＤとパワーを入力するために必要とされる画面情報を加入者端末２０１に送信する。ここで“ｈｔｔｐ”手順とは、ＨＴＭＬ（Hyper Text Markup Language）転送のためのハイパーテキスト転送プロトコルとして規定された要求と返答を組み合わせた手順をいう。画面情報の送信によって、加入者端末２０１は認証のためのユーザＩＤとパワーを入力する画面を表示することができる。

【００４９】

この画面の表示状態で加入者は加入者端末２０１を操作して、ユーザＩＤとパスワードを“ｈｔｔｐ”手順で入力する。ログイン用ウェブサーバ２１５は“ｈｔｔｐ”手順でアクセスしてきた加入者端末２０１のＩＰアドレスを管理用ＩＰネットワーク２１２を経由してデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６に渡す。デフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６は加入者端末２０１のＩＰアドレスを受け取ると、そのＩＰアドレスに対応する加入者端末２０１のＭＡＣアドレスをログイン用ウェブサーバ２１５に通知する。ログイン用ウェブサーバ２１５は加入者端末２０１のＭＡＣアドレスの通知を受けると、これと先に受け取ったユーザＩＤおよびパスワードを、管理用ＩＰネットワーク２１２を経由して第１および第２のＲＡＤＩＵＳサーバ213_1、213_2のうち該当するものへ渡して認証の依頼を行う。

【００５０】

今、加入者端末２０１がインターネットの接続について契約を行っている第１のインターネットサービスプロバイダ208_1に関しては、第１のＲＡＤＩＵＳサーバ213_1がこれを担当することになる。なお、第２のＲＡＤＩＵＳサーバ213_2は第１のＲＡＤＩＵＳサーバ213_1と基本的に同一の構成となっているため、その動作についての説明は省略する。

【００５１】

この例の場合、第１のＲＡＤＩＵＳサーバ213_1は、ログイン用ウェブサーバ２１５から受け取ったユーザＩＤとパスワードを認証する。そしてその結果をログイン用ウェブサーバ２１５に通知する。このとき、第１のＲＡＤＩＵＳサーバ213_1はユーザＩＤとＭＡＣアドレスとを図示しない記憶領域に記憶しておく。

【００５２】

ログイン用ウェブサーバ２１５は、第１のＲＡＤＩＵＳサーバ213_1から認証結果を受け取る。パスワードが一致しない等の理由で認証が失敗であれば、ログイン用ウェブサーバ２１５はその旨を示す画面を“ｈｔｔｐ”手順で加入者端末２０１に送り込む。認証が成功であれば、成功であることを示す画面を同様に“ｈｔｔｐ”手順で加入者端末２０１に送り込む。また、認証が成功の場合、ロ

グイン用ウェブサーバ２１５は物理ポート切替スイッチ２０４に対して、今後この加入者端末２０１のＭＡＣアドレスを有するパケット信号を受け取った場合にはこれを認証ポート２０５と接続された認証ＩＰネットワーク２０７にフォワードするように指示を送出する。

【００５３】

この指示を受けた物理ポート切替スイッチ２０４は、前記したＭＡＣアドレス登録テーブルにそのＭＡＣアドレスを登録する。そして、加入者端末２０１がログアウトしない限り、同一のＭＡＣアドレスを持ったパケット信号が到来したとき、認証ポート２０５に接続された認証ＩＰネットワーク２０７にフォワードするように動作することになる。

【００５４】

このようにして加入者端末２０１がこれ以後、ローカルエリアネットワーク２０２に送出するパケット信号は物理ポート切替スイッチ２０４を介して認証ＩＰネットワーク２０７にフォワードされるが、ＩＰアドレスのリース時間は有限である。そこで、加入者端末２０１はリース時間ｔの２分の１の時間が経過すると（ステップＳ５０４）、リースの延長を求めるＤＨＣＰリクエストパケットを送出する（ステップＳ５０５）。このＤＨＣＰリクエストパケットはユニキャストフレームとして送信される。臨時のＩＰアドレスが発行されたこの時点ではデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６を宛先として送出される。

【００５５】

このＤＨＣＰリクエストに対して、該当するデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６から“ａｃｋ”信号が返却されてきたときには（ステップＳ５０６：Ｙ）、そのデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６はその時点でリース時間ｔを再延長している。したがって、加入者端末２０１はリース時間ｔの２分の１の時間が経過するたびに同じ動作を繰り返すようにすることでリース時間ｔを何回でも延長することができる。このようなリース時間ｔが設けられている主旨は、加入者端末２０１がログアウトをしても同一のＩＰアドレスを保持する事態を避けて、予め用意したＩＰアドレスが枯渇することを防止するためである。

【００５６】

ところで、加入者端末２０１がステップＳ５０５でリースの延長を求めるＤＨＣＰリクエストパケットを送出したにも係わらず該当するデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６が何らかの原因で“ａｃｋ”信号を返送しない場合がある（ステップＳ５０６：Ｎ）。このような場合には、リース時間ｔの８分の７の時間が経過する前までは（ステップＳ５０７：Ｙ）、ステップＳ５０５に戻ってユニキャストフレームでＤＨＣＰリクエストパケットを繰り返し送出する。

【００５７】

このようにＤＨＣＰリクエストパケットを繰り返し送出しても、該当するデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６から“ａｃｋ”信号が送り返されない場合には（ステップＳ５０７：Ｎ）、リース時間ｔの８分の７の時間に到達した時点で（ステップＳ５０７：Ｎ）、今度はブロードキャストフレームでＤＨＣＰリクエストパケットを送出する（ステップＳ５０８）。これにより、このＤＨＣＰリクエストはデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６だけでなく認証ＩＰネットワークＤＨＣＰサーバ２１１にも伝達されることになる。

【００５８】

このＤＨＣＰリクエストに対して認証ＩＰネットワークＤＨＣＰサーバ２１１から“ａｃｋ”信号が送り返された場合には（ステップＳ５０９：Ｙ）、リース時間ｔが更新される。これにより処理はステップＳ５０４に戻ることになる。これに対して“ａｃｋ”信号が送り返されてこなかったような場合には（ステップＳ５０９：Ｎ）、リース時間ｔが切れるまで（ステップＳ５１０：Ｎ）、ブロードキャストフレームでＤＨＣＰリクエストパケットを繰り返し送出する（ステップＳ５０８）。そして、リース時間ｔが切れた時点で（ステップＳ５１０：Ｙ）、そのＩＰアドレスを開放することになる（ステップＳ５１１）。

【００５９】

ところで、認証ＩＰネットワークＤＨＣＰサーバ２１１はＤＨＣＰ手順によって加入者端末２０１のＭＡＣアドレスを知ることができる。そこで認証ＩＰネットワークＤＨＣＰサーバ２１１は管理用ＩＰネットワーク２１２を経由して担当

の第１のＲＡＤＩＵＳサーバ２１３$_1$に加入者端末２０１のＭＡＣアドレスを渡して、これに対して割り当てるべき適切なＩＰアドレスを通知するように依頼する。

【００６０】

第１のＲＡＤＩＵＳサーバ２１３$_1$はこの依頼を受けると、認証ＩＰネットワークＤＨＣＰサーバ２１１から加入者端末２０１のＭＡＣアドレスを受け取り、先に記憶しておいたユーザＩＤとＭＡＣアドレスの組み合わせから対応するユーザＩＤを取り出す。そしてこのユーザＩＤに割り当てるべきＩＰアドレスを決定し、認証ＩＰネットワークＤＨＣＰサーバ２１１に対してこの決定したＩＰアドレスを通知する。なお、このＩＰアドレスは第１のＲＡＤＩＵＳサーバ２１３$_1$が事前にストックしておいたアドレスの中から払い出すものであるが、これに限るものではない。たとえはデフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６が臨時で与えたＩＰアドレスをそのまま与えても差し支えない。ただし、デフォルトＩＰネットワーク用ＤＨＣＰサーバ２１６が臨時で与えるＩＰアドレスは、ネットワークサービスプロバイダ２０３内で他のＩＰアドレスと競合するものでなければどのようなものでもよいが、第１のＲＡＤＩＵＳサーバ２１３$_1$や第２のＲＡＤＩＵＳサーバ２１３$_2$が払い出すＩＰアドレスはネットワークサービスプロバイダ２０３の外でも同一のものが無いことが条件となる。

【００６１】

認証ＩＰネットワークＤＨＣＰサーバ２１１は、割り当てるべきＩＰアドレスを、この例の場合、第１のＲＡＤＩＵＳサーバ２１３$_1$から通知されると、加入者端末２０１からのＤＨＣＰリクエストパケットに対してＩＰアドレスを割り当てたことを通知する割当通知パケットを返送する。

【００６２】

ところでＩＰサブネット振分スイッチ２０９は、認証ＩＰネットワーク２０７からＩＰパケットが送られてくると、レイヤ３のＩＰサブネットワークアドレスをチェックして、それぞれ該当するＩＰネットワークへフォワードするようにこれらの対応関係をスタティックに設定している。その結果、たとえば第１のターゲットＩＰネットワーク２１４$_1$のサブネットワークに一致したサブネットワー

クアドレスのＩＰパケットが到来すればこれを第１のターゲットＩＰネットワーク２１４$_1$へフォワードする。また、第２のターゲットＩＰネットワーク２１４$_2$のサブネットワークに一致したサブネットワークアドレスのＩＰパケットが到来すればこれを第２のターゲットＩＰネットワーク２１４$_2$へフォワードすることになる。

【００６３】

先の例では、加入者端末２０１がインターネット網へのアクセスについて第１のインターネットサービスプロバイダ２０８$_1$と契約している。したがって、第１のＲＡＤＩＵＳサーバ２１３$_1$が加入者端末２０１用のＩＰアドレスを与えることになる。このＩＰアドレスのパケット信号はＩＰサブネット振分スイッチ２０９で第１のターゲットＩＰネットワーク２１４$_1$の第１のインターネットサービスプロバイダ２０８$_1$に送られ、これを経由して図示しないインターネット網に転送されることになる。

【００６４】

＜第２の実施例＞

【００６５】

図５は、本発明の第２の実施例におけるユーザ認証システムを表わしたものである。このユーザ認証システム６００は、ある会社が社員や協力会社のスタッフのそれぞれにアクセスできるローカルエリアネットワークを振り分けるようにした認証システムである。ユーザ認証システム６００は、パーソナルコンピュータからなる第１～第Ｎの入出力端末６０１$_1$～６０１$_N$と、これらに共通して接続された社内一般向けローカルエリアネットワーク（ＬＡＮ）６０２と、特殊目的あるいは用途の第１～第Ｍの専門別ローカルエリアネットワーク６０３$_1$～６０３$_M$と、これら第１～第Ｍの専門別ローカルエリアネットワーク６０３$_1$～６０３$_M$に対する認証と振分けを行う認証・振分け装置６０４とから構成されている。

【００６６】

ここで、認証・振分け装置６０４は社内一般向けローカルエリアネットワーク６０２と接続された物理ポート切替スイッチ６１１を備えている。物理ポート切替スイッチ６１１は認証の行われたユーザの一覧を登録するユーザ登録テーブル

６１２を備えている。ユーザ登録テーブル６１２はユーザが第１～第Mの専門別ローカルエリアネットワーク６０３$_1$～６０３$_M$のうちの特定のものにログインする要求を行って認証が成功したときに登録され、その専門別ローカルエリアネットワーク６０３からログアウトしたときに登録を消去されるようになっている。

【００６７】

物理ポート切替スイッチ６１１はこのユーザ登録テーブル６１２の他に先の実施例と同様の未認証ポート６１３と認証ポート６１４を備えている。ユーザ登録テーブル６１２に登録されていないユーザからアクセスがあったときには未認証ポート６１３が選択され、送られてきたブロードキャストアドレスのパケットはこの未認証ポート６１３に接続された未認証用ネットワーク６１６に転送される。未認証用ネットワーク６１６には、ログイン用ウェブサーバ６１７とデフォルトアドレスサーバ６１８が接続されている。これらログイン用ウェブサーバ６１７とデフォルトアドレスサーバ６１８は管理用ネットワーク６１９にも接続されている。

【００６８】

一方、認証ポート６１４には認証用ネットワーク６２１が接続されている。認証用ネットワーク６２１にはユーザが第１～第Mの専門別ローカルエリアネットワーク６０３$_1$～６０３$_M$のうちのいずれか希望するものにログインするための認証を行う認証サーバ６２２と、アドレス振分スイッチ６２３が接続されている。アドレス振分スイッチ６２３はユーザから送られてきたパケット信号のサブアドレスに応じて第１～第Mの専門別ローカルエリアネットワーク６０３$_1$～６０３$_M$のいずれかにこのパケット信号を振り分けて送出するようになっている。認証サーバ６２２は管理用ネットワーク６１９にも接続されている。また、管理用ネットワーク６１９にはこれ以外にサブアドレス付与サーバ６２４が接続されている。サブアドレス付与サーバ６２４は認証されたパケット信号のユーザに対して希望する専門別ローカルエリアネットワーク６０３に対応したサブアドレスを付与するようになっている。

【００６９】

このようなユーザ認証システム６００で、たとえば光ファイバの研究者である

ユーザＡが社内の光ファイバに関する技術情報を集めた第１の専門別ローカルエリアネットワーク６０３$_1$にアクセスする場合を例にとって説明する。ユーザＡは自己の社員証の磁気情報を第１～第Ｎの入出力端末６０１$_1$～６０１$_N$のいずれかに接続された図示しない磁気情報読取装置から読み取らせる。この情報を組み込んだパケット信号は、認証・振分け装置６０４の物理ポート切替スイッチ６１１に入力される。

【００７０】

物理ポート切替スイッチ６１１ではこのパケット信号に組み込まれた磁気カードの読取情報をキーとしてユーザ登録テーブル６１２を検索し、未認証であることを知る。そこで、このパケット信号は未認証ポート６１３から未認証用ネットワーク６１６に転送される。デフォルトアドレスサーバ６１８はこのパケット信号を受信するとこのユーザＡに臨時で対応するＩＰアドレスを発行する。このＩＰアドレスはパケット信号の送信元のユーザＡに返送される。ユーザＡはこのＩＰアドレスを使用したパケット信号を認証要求のために送信し、ログイン用ウェブサーバ１７によって一般的なブラウザによって認証用の画面が表示される。ユーザＡはこの状態で、ログインする希望の第１の専門別ローカルエリアネットワーク６０３$_1$の名称と自己のパスワードを入力することになる。

【００７１】

この入力情報は先の磁気情報と共に認証サーバ６２２に与えられる。認証サーバ６２２は第１～第Ｍの専門別ローカルエリアネットワーク６０３$_1$～６０３$_M$のそれぞれに対する社員ごとのアクセス権限を記したテーブルを参照し、認証の可否を決定する。認証が成功したときにはサブアドレス付与サーバ６２４がユーザＡの希望した第１の専門別ローカルエリアネットワーク６０３$_1$に対応したサブアドレスをユーザＡ用に設定する。このサブアドレスは認証成功の通知と共に社内一般向けローカルエリアネットワーク６０２を経てユーザＡに返送される。また、認証が成功した時点でユーザ登録テーブル６１２にユーザＡが登録される。

【００７２】

この後、ユーザＡが第１の専門別ローカルエリアネットワーク６０３$_1$に向けたパケット信号を送出すると、物理ポート切替スイッチ６１１はこれを認証ポー

ト６１４から認証用ネットワーク６２１に向けて送り出す。このパケット信号はアドレス振分スイッチ６２３に入力される。アドレス振分スイッチ６２３はパケット信号のサブアドレスを見て、このパケット信号を第１の専門別ローカルエリアネットワーク６０３_{1}に転送することになる。

【００７３】

なお、以上説明した第１の実施例では付与されたＩＰアドレスのサブアドレスを用いてターゲットＩＰネットワークを振り分ける処理を行ったが、そのパケット信号のＭＡＣアドレスを併せて使用して、たとえば両者が一致する通信ネットワークに対してパケット信号の振り分けを行うことも可能である。これにより、ＩＰアドレスを使用しただけの場合と比べて第三者が不用意にＩＰネットワークに侵入する事態を回避し、セキュリティを向上させることができる。

【００７４】

また、第１の実施例では付与されたＩＰアドレスのサブアドレスを用いてパケット信号の振り分けを行ったが、ＭＡＣアドレスのみで振り分けを行うことも可能である。

【００７５】

【発明の効果】

以上説明したように請求項１記載の発明によれば、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力し、これが認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与えると共にログイン画面表示手段でログインの際の画面表示を行うようにした。これにより、通信端末にインターネット上の情報を表示するために一般的に備えられているブラウザを使用してログイン操作が可能になる。すなわち、ログインのために特別のソフトウェアを通信端末にインストールする必要がない。また、認証が成功した場合には一時使用ＩＰアドレスに代えて認証の対象となった所望の通信ネットワークに転送するためのネットワークアドレスが与えられるので、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。ネットワークアドレスの数は前記したＶＬＡＮフィールドのビット数に

よる制限がないので、通信システムの構築の自由度が拡大する。また、ネットワークアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【００７６】

また、請求項２記載の発明によれば、ネットワーク振り分け手段を備えているので、通信端末が与えられたネットワークアドレスを使用することで単純にパケット信号の振り分けを行うことができる。

【００７７】

更に請求項３記載の発明によれば、通信端末が送出したパケット信号を、認証を要する所定の通信ネットワークの手前に配置された物理ポート切替手段が入力し、これが認証済でない場合にはそのパケット信号を送出した通信端末に対してログイン用の一時使用ＩＰアドレスを一時的に与えると共にログイン画面表示手段でログインの際の画面表示を行うようにした。これにより、通信端末にインターネット上の情報を表示するために一般的に備えられているブラウザを使用してログイン操作が可能になる。すなわち、ログインのために特別のソフトウェアを通信端末にインストールする必要がない。また、認証が成功した場合には一時使用ＩＰアドレスに代えて正規のＩＰアドレスを与えるので、それ以後は物理ポート切替手段の認証済ポートを介して所望の通信ネットワークとの通信が可能になる。ＩＰアドレスの数は前記したＶＬＡＮフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。また、ネットワークアドレスによってパケット信号の宛先を処理するので、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。

【００７８】

また請求項４記載の発明によれば、ＩＰサブネット振り分け手段を備えているので、通信端末が与えられたＩＰアドレスを使用することで単純にパケット信号の振り分けを行うことができる。

【００７９】

更に請求項６記載の発明によれば、ＩＰサブネット振り分け手段は、ＩＰアドレスと通信端末のＭＡＣアドレスのいずれかを用いて通信端末から送られてきたパケット信号の振り分けを行うので、異なった観点からパケット信号の振り分けを行うことができる。

【００８０】

また請求項７記載の発明によれば、通信端末からアクセスがあったときこれに対してインターネットでアクセス可能なアドレスを与えてウェブ表示画面を用いて認証の手続きを行うので、通信端末に特別な認証用のアプリケーションソフトウェアをインストールすることなく、通常備わっているブラウザを使用して認証のための操作が可能である。

【００８１】

更に請求項８記載の発明によれば、ＩＰサブネット振り分け手段は、ＩＰアドレスとＭＡＣアドレスの双方が一致したことをもってパケット信号の振り分け先を決めることにしたので、アクセスに対するセキュリティを高めることが可能になる。

【００８２】

また請求項９記載の発明によれば、一時使用ＩＰアドレス返送ステップで一時使用ＩＰアドレスを通信端末に返送し、これを使用させて認証要求を行わせることにしたので、この一時使用ＩＰアドレスを使用して認証のための手続きをインターネットサービスプロバイダの手前側で簡易に処理することができる。また、個々のインターネットサービスプロバイダ用にＩＰアドレスを振り分けておくことで、通信端末側から送られてきたパケット信号のＩＰアドレスを判読することでどのインターネットサービスプロバイダに振り分けるかを簡易に判別することができ、ポイントツーポイントプロトコルを使用した技術と比較して処理が単純化し、スループットが低下することはない。しかもＩＰアドレスの数は前記したＶＬＡＮフィールドのビット数による制限がないので、通信システムの構築の自由度が拡大する。

【図面の簡単な説明】

【図１】

本発明の第１の実施例におけるユーザ認証システムを表わしたシステム構成図である。

【図２】

本実施例の物理ポート切替スイッチの制御の様子を表わした流れ図である。

【図３】

本実施例のユーザ認証システムにおける認証およびパケット信号の振り分けの原理を示した説明図である。

【図４】

ＤＨＣＰリクエストパケットが送出された時点以降の本実施例のユーザ認証システムにおける加入者端末側の処理の概要を表わした流れ図である。

【図５】

本発明の第２の実施例におけるユーザ認証システムを表わしたシステム構成図である。

【図６】

ＡＤＳＬを使用してネットワークサービスプロバイダに接続する従来の通信システムの概要を表わしたシステム構成図である。

【図７】

ポイントツーポイントプロトコルを使用しないで済む従来提案された通信システムの概要を表わしたシステム構成図である。

【符号の説明】

２００、６００　ユーザ認証システム

２０１　加入者端末

２０２　ローカルエリアネットワーク

２０４、６１１　物理ポート切替スイッチ

２０５　認証ポート

２０６　未認証ポート

２０７　認証ＩＰネットワーク

２０９　ＩＰサブネット振分スイッチ

２１１　認証ＩＰネットワークＤＨＣＰサーバ

２１２　管理用ＩＰネットワーク

２１３　ＲＡＤＩＵＳサーバ

２１４　ターゲットＩＰネットワーク

２１５、６１７　ログイン用ウェブサーバ

２１６　デフォルトＩＰネットワーク用ＤＨＣＰサーバ

２１７　デフォルトＩＰネットワーク

４０１　パケット信号

４０２　ユーザ認証手段

４０３　ＩＰサブネットアドレス払出手段

４０４　ＩＰアドレスＭＡＣアドレスフィルタ手段

４０５　振分手段

６０１　入出力端末

６０２　社内一般向けローカルエリアネットワーク

６０３　専門別ローカルエリアネットワーク

６０４　認証・振分け装置

６１８　デフォルトアドレスサーバ

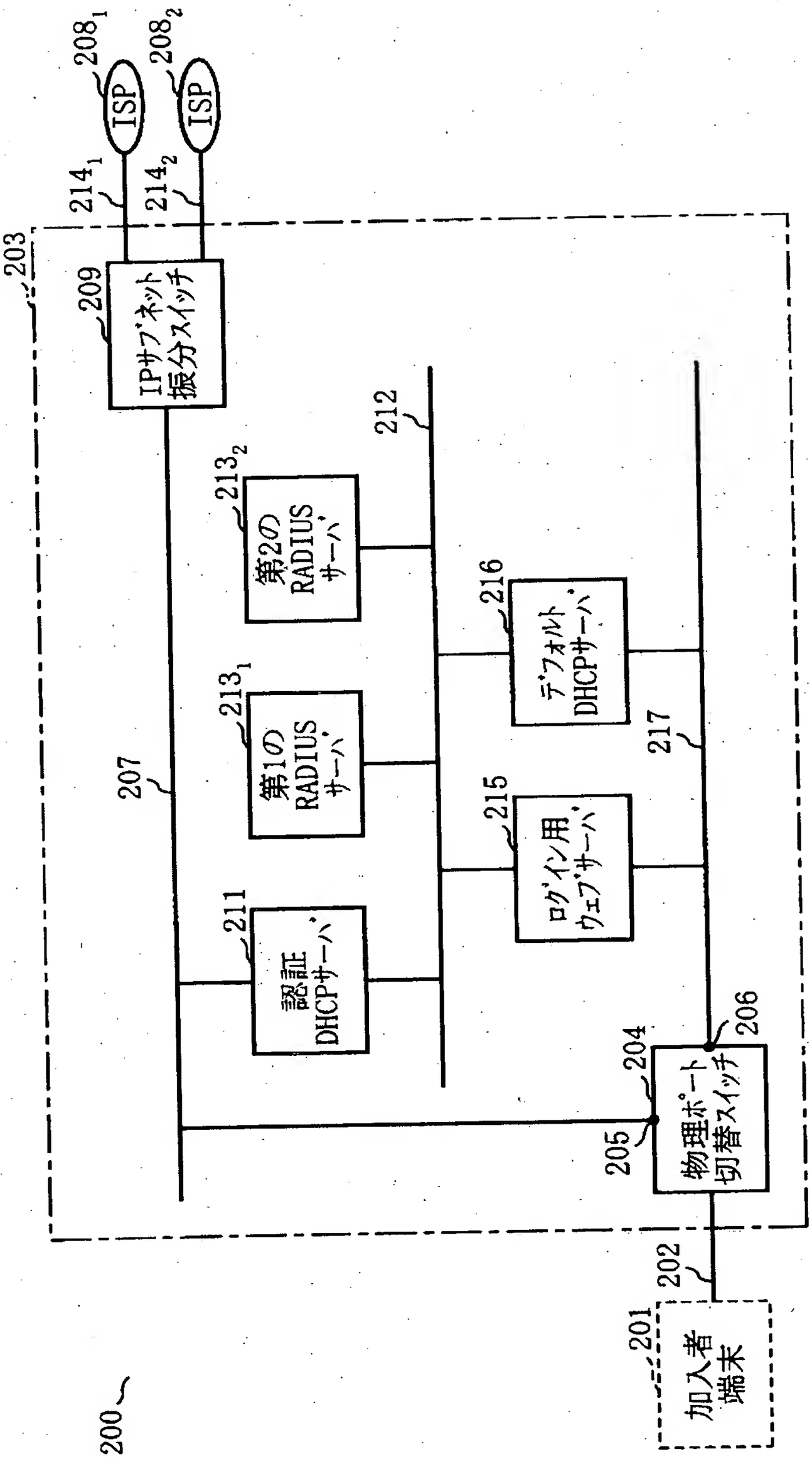
６２２　認証サーバ

６２３　アドレス振分スイッチ

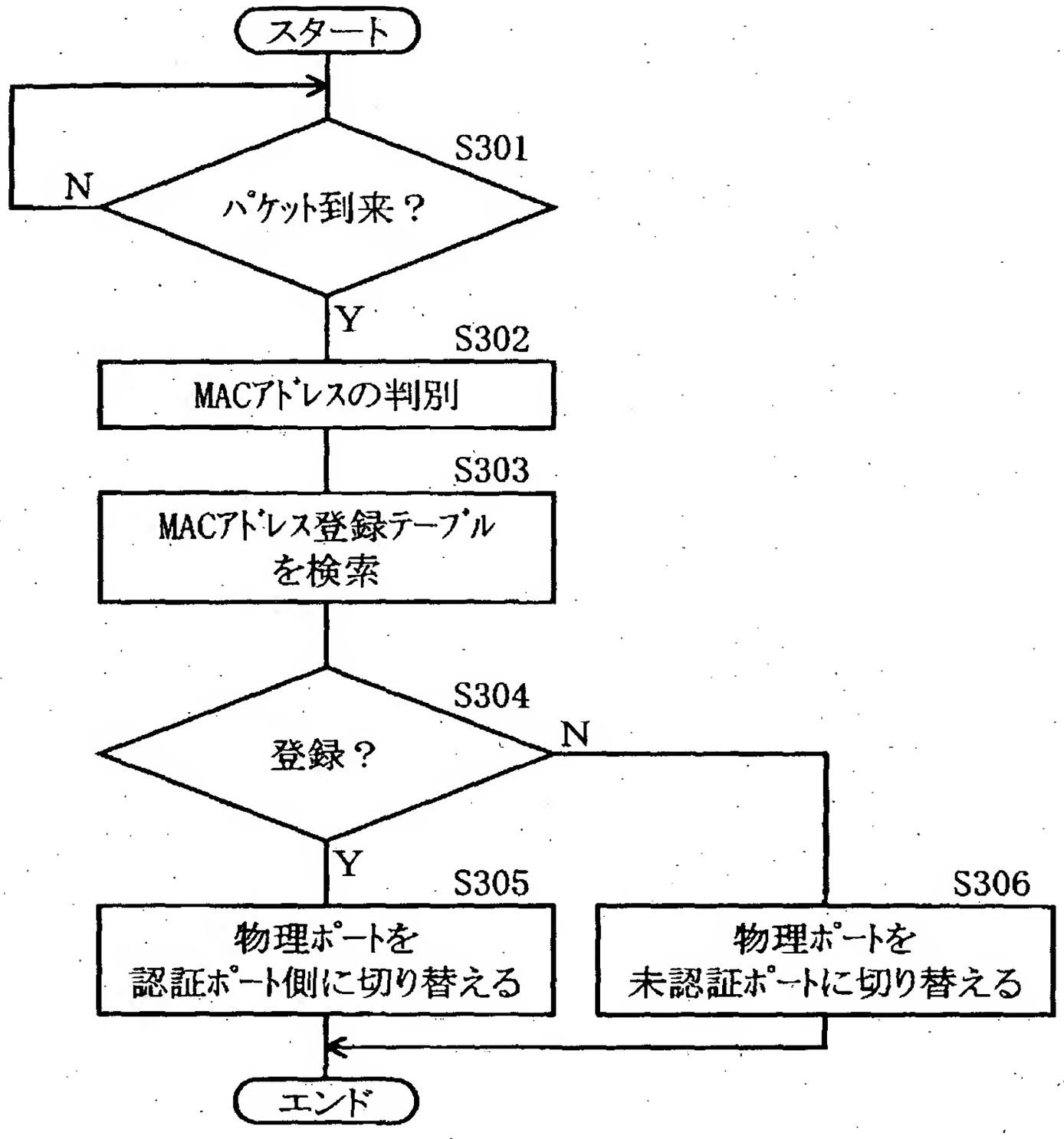
６２４　サブアドレス付与サーバ

【書類名】　図面

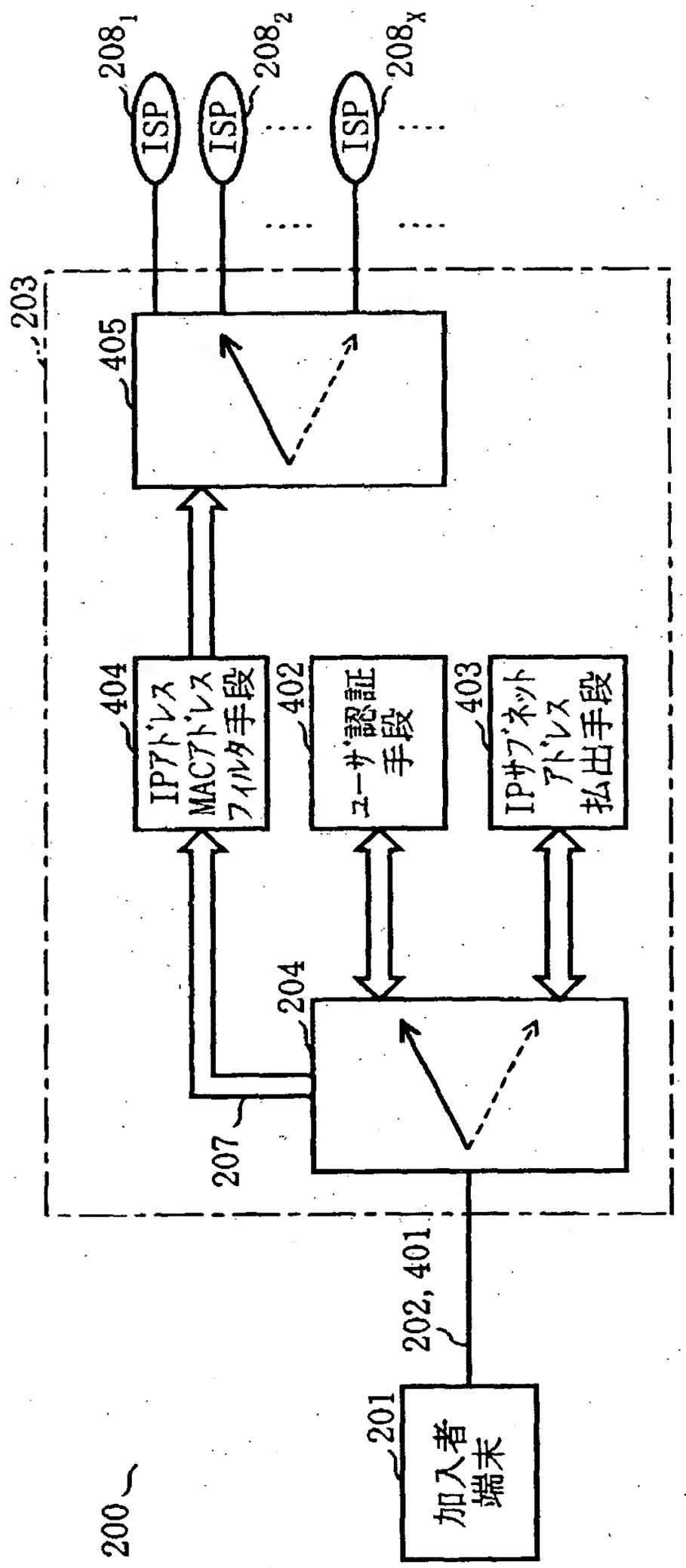
【図１】


200
201
加入者端末
202
物理ポート切替スイッチ
204
205
206
207
IPサブネット振分スイッチ
209
211
認証DHCPサーバ
212
213₁
第1のRADIUSサーバ
213₂
第2のRADIUSサーバ
214₁
214₂
ISP
ISP
208₁
208₂
215
ログイン用ウェブサーバ
216
デフォルトDHCPサーバ
217

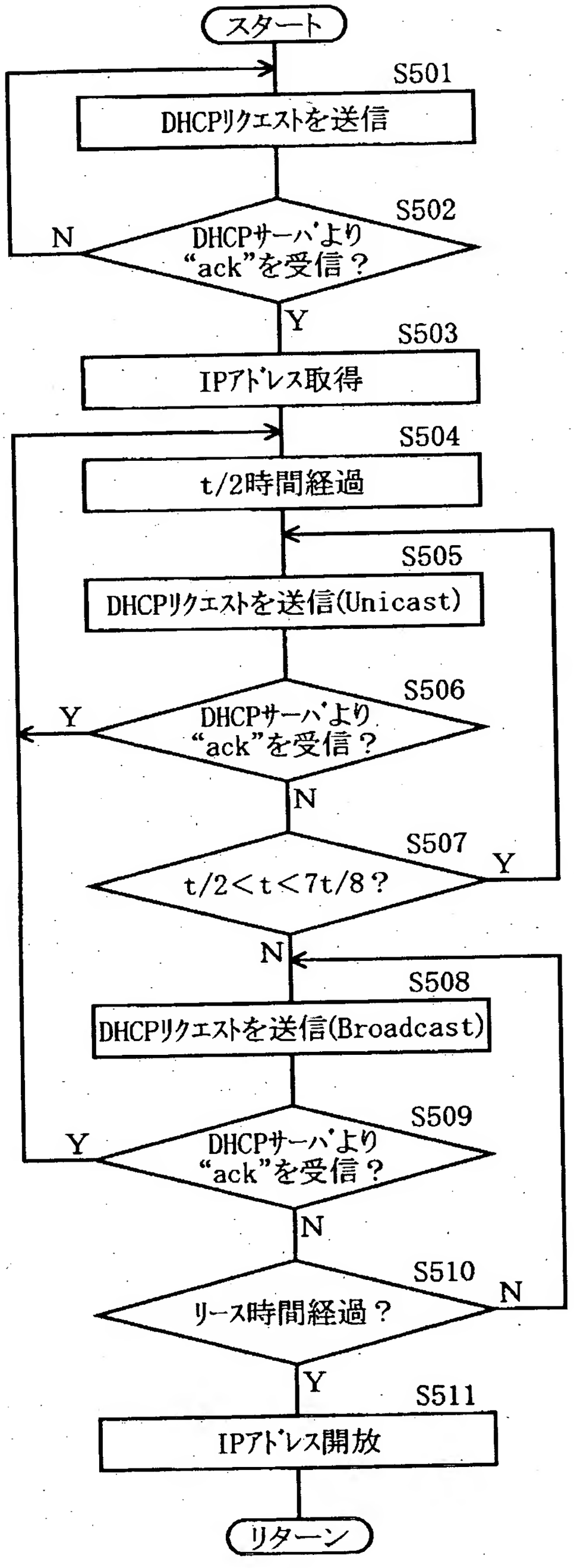
【図２】


スタート
S301
パケット到来？
N
Y
S302
MACアドレスの判別
S303
MACアドレス登録テーブル
を検索
S304
登録？
N
Y
S305
物理ポートを
認証ポート側に切り替える
S306
物理ポートを
未認証ポートに切り替える
エンド

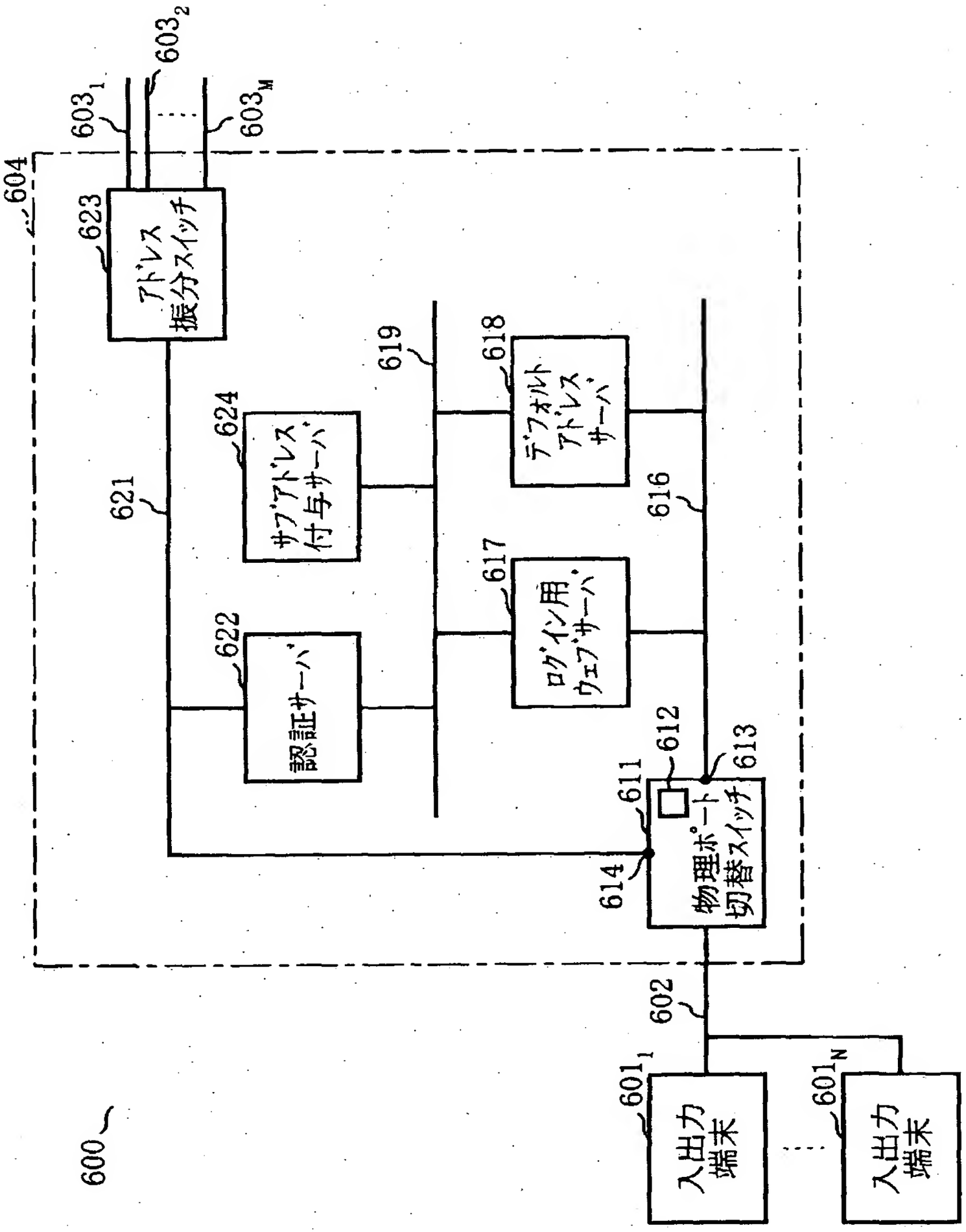
【図３】


208$_1$
208$_2$
208$_X$
ISP
ISP
ISP
203
405
404
IPアドレス
MACアドレス
フィルタ手段
402
ユーザ認証
手段
403
IPサブネット
アドレス
払出手段
204
207
202, 401
201
加入者
端末
200

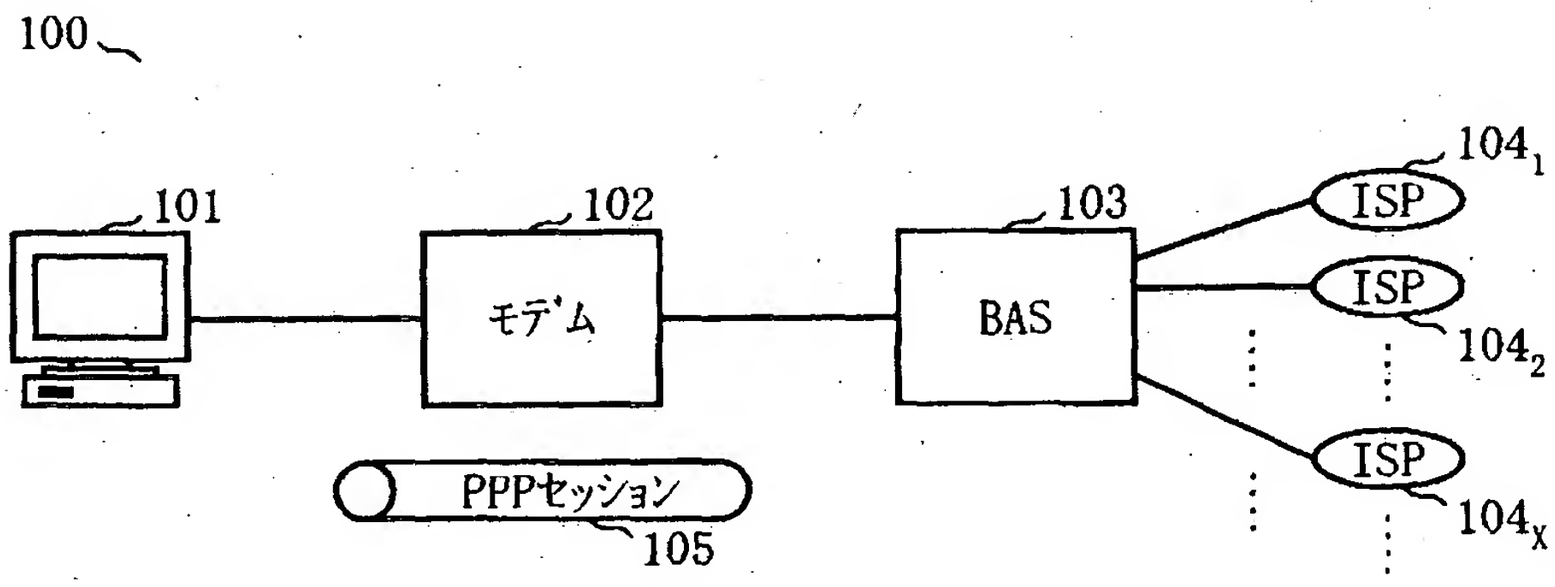
【図４】


スタート
S501
DHCPリクエストを送信
S502
DHCPサーバより“ack”を受信？
N
Y
S503
IPアドレス取得
S504
t/2時間経過
S505
DHCPリクエストを送信(Unicast)
S506
DHCPサーバより“ack”を受信？
Y
N
S507
t/2＜t＜7t/8？
Y
N
S508
DHCPリクエストを送信(Broadcast)
S509
DHCPサーバより“ack”を受信？
Y
N
S510
リース時間経過？
N
Y
S511
IPアドレス開放
リターン

【図５】


600
604
603₁
603₂
603M
623
アドレス振分スイッチ
621
624
サブアドレス付与サーバ
619
618
デフォルトアドレスサーバ
616
622
認証サーバ
617
ログイン用ウェブサーバ
611
612
613
614
物理ポート切替スイッチ
602
601₁
601N
入出力端末
入出力端末

【図６】


100
101
102
モデム
103
BAS
104₁
ISP
ISP
104₂
ISP
104X
PPPセッション
105

【図７】


120
101
121
VLAN
スイッチ
122$_1$
122$_2$
122$_X$
ISP
ISP
ISP
104$_1$
104$_2$
104$_X$

【書類名】　　要約書

【要約】

【課題】　通信端末がローカルエリアネットワーク（ＬＡＮ）を介して自在に通信ネットや所望のＬＡＮに数の制約なく接続することのできるユーザ認証システムおよびユーザ認証方法を得る。

【解決手段】　加入者端末２０１はＬＡＮ２０２およびネットワークサービスプロバイダ２０３内のＩＰサブネット振分スイッチ２０９を介してインターネットサービスプロバイダ２０８に接続される構成となっている。物理ポート切替スイッチ２０４は未認証のパケット信号を入力すると臨時のＩＰアドレスを加入者端末２０１に与え、これを用いて認証処理を行わせる。認証が成功したら正規のＩＰアドレスが付与され、これを使用したパケット信号はＩＰサブネット振分スイッチ２０９によって目的のネットワークに振り分けられる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００２－２００９２０
受付番号	５０２０１００８４２５
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１４年　７月１１日

＜認定情報・付加情報＞

【提出日】　平成14年 7月10日

次頁無

出　願　人　履　歴　情　報

識別番号　〔０００００４２３７〕

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社